REMARKS

This amendment is in response to the office action dated June 20, 2006. Claims 1,2, 4-36 and 38 were pending in the application as of this office action, including independent claims 1, 26, 32 and 34-36.

Claims 18-22, 30, 31 and 38 are objected to as depending from rejected base claims, but are otherwise allowable.

Claims 1, 26, 34 and 35 have been amended. No new matter has been added.

Reexamination and reconsideration of the action are requested in light of the foregoing amendments and the following remarks.

Section 102 Rejections

A. *Claims 1, 11, 13-16, 23 and 34 stand rejected under 35 U.S.C. 102(e) as being allegedly anticipated by U.S. Pat. No. 6,772,340 ("Peinado").*

Claim 1 recites, in part, that an encrypted first key is provided in an access controlled manner to users for use in opening an encrypted document. A second key, associated with the first key, is provided in a second access controlled manner to users for use in opening all documents that can be opened through use of the first key. The second access controlled manner is distinct from the first access controlled manner.

Claim 1 requires that the first key and the second key are provided in distinct access controlled manners. In contrast, Peinado discloses only one key access control mechanism: an end-user license:

> Once the downloaded license has been stored in the DRM system license store, the user can render the digital content according to the rights conferred by the license and specified in the license terms. When a request is made to render the digital content, the black box is caused to decrypt the decryption key and license terms, and a DRM system license evaluator evaluates such license terms. The black box decrypts the encrypted digital content only if the license evaluation results in a decision that the requestor is allowed to play such content. The decrypted content is provided to the rendering application for rendering. *See* col. 3, lines 57-67.

Accordingly, the applicant submits that claim 1 and its dependent claims are in condition for allowance. Claim 34 is directed to a program product but otherwise incorporates limitations that are similar to those of claim 1 and is therefore in condition for allowance for at least the same reason.

Section 103 Rejections

A. *Claim 2 stands rejected under 35 U.S.C. 103(a) as being allegedly unpatentable over Peinado in view of U.S. Pat. No. 6,336,189 ("Takeda").*

Claim 2 depends from claim 1. The cited portions of Takeda do not overcome the deficiencies of Peinado with respect to claim 1, as addressed above. Neither the cited portions of Peinado nor those of Takeda disclose providing a second key in a second access controlled manner for use in opening all documents that can be opened through use of the first key provided in a first access controlled manner where the second and first access controlled manners are distinct, as recited in claim 1. Therefore Takeda does not overcome the deficiencies of Peinado and claim 2 is also in condition for allowance for at least the reasons addressed above in reference to claim 1.

B. *Claims 4-7, 17, 32, 33 and 36 are rejected under 35 U.S.C. 103(a) as being allegedly unpatentable over Peinado in view of U.S. Pat. No. 6,069,957 ("Richards").*

Claims 4-7, 17, 32, 33 and 36. Claims 4-7 and 17 depend from claim 1. The cited portions of Richards do not overcome the deficiencies of Peinado with respect to claim 1. Therefore, claims 4-7 and 17 are also in condition for allowance for at least the same reasons as claim 1.

Claim 32 recites in part, a single skeleton key can be opened using one or more other skeleton keys. The examiner asserts on page 5 of the action that:

> Richard further discloses using a key (CUSTOMER_CODE) to encrypt SK (col. 6:63) or a key (PK) to encrypt SK (col. 9:14-18) which anticipates the limitation a single skeleton key can be opened using one or more other skeleton keys.

The applicant disagrees. The CUSTOMER_CODE key is not itself encrypted, only "extremely well concealed." *See* col. 10, lines 56-64. Thus, the CUSTOMER_CODE key

cannot be opened using one or more skeleton keys. Hence, the CUSTOMER_CODE key is not a skeleton key. The PK key is also not a skeleton key since the PK key is opened using the CUSTOMER_CODE key, which is not a skeleton key. *See* col. 9, lines 19-25. Finally, the SK key is not a skeleton key since it is opened with two keys that are not skeleton keys, i.e., the CUSTOMER_CODE key and the PK key.

The relied upon portions of Peinado do not remedy the deficiencies of Richards.

For at least these reasons, the applicant submits that claim 32 and its dependent claim are in condition for allowance. Claim 36 incorporates a similar limitation and is in condition for allowance for at least the same reasons.

C. *Claims 8-10, 12, 24-29 and 35 are rejected under 35 U.S.C. 103(a) as being allegedly unpatentable over Peinado and further in view of Stallings, Cryptography and Network Security ("Stallings").*

Claims 8-10, 12 and 24-25 depend from claim 1. The cited portions of Stallings do not overcome the deficiencies of Peinado with respect to claim 1. Therefore, claims 8-10, 12 and 24-25 are in condition for allowance for at least the same reasons as claim 1.

Claim 26 recites in part, at least one association is a pair consisting of the encrypted second key and an encrypted third key, the association indicating that the decrypted second key can be used to decrypt and thereby make usable the third key.

The examiner concedes that Peinado does not explicitly disclose defining such associations. *See* p. 16 of the Office Action mailed June 20, 2006. The cited portion of Stallings describes sending an identifier Key ID for a public key KU_b in a message containing encrypted data so that a receiver of a message (usually) knows what private key to use to decrypt a session key K_s. *See* Stallings, pp. 363-364 and Fig. 12.3. Stallings' discloses a key ring that contains keys. Each key on the key ring is unassociated to other keys on the key ring except that they exist in the same collection. Although a Key ID, for the sake of argument, may constitute an association between a key on the key ring and a message's session key, there is no association between the decrypted session key and a third key.

In fact, the session key is not used to decrypt anything other than the message to which it is attached, in particular, "[e]ach session key is associated with a single message and is used only

for the purpose of encrypting and decrypting that message." *See* Stallings, p. 363, first paragraph under 'Session Key Generation' (*emphasis added*). Therefore, the cited portions of Stallings do not disclose or suggest that the decrypted second key can be used to decrypt a third key, as recited in claim 26.

For at least this reason, the applicant respectfully submits that claim 26 and its dependants are in condition for allowance.

Claim 35 incorporates similar limitations as claim 26 and is in condition for allowance for at least the reasons addressed in reference to claim 26.

Conclusion

By responding in the foregoing remarks only to particular positions taken by the examiner, the Applicant does not acquiesce with other positions that have not been explicitly addressed. In addition, the Applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist.

The Applicant respectfully requests that all pending claims be allowed. Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 11/20/2006

Daniel J. Burns
Reg. No. 50,222

Customer No. 021876
Fish & Richardson P.C.
Telephone: (650) 839-5070
Facsimile: (650) 839-5071